PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04J 14/00, 14/02, H04K 1/02, 1/10

A1

(11) International Publication Number: **WO 00/30281**

(43) International Publication Date: 25 May 2000 (25.05.00)

(21) International Application Number: PCT/US99/26529

(22) International Filing Date: 10 November 1999 (10.11.99)

(30) Priority Data:
60/108,127 12 November 1998 (12.11.98) US

(71) Applicant: TELCORDIA TECHNOLOGIES, INC. [US/US]; 445 South Street, Morristown, NJ 07960–6438 (US).

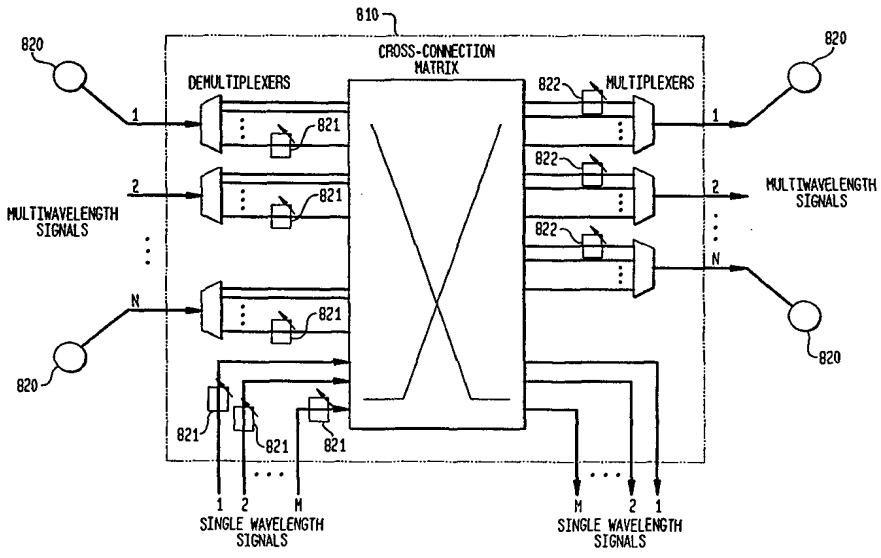
(72) Inventor: ETEMAD, Shahab; 2 Crest Lane, Warren, NJ 07059 (US).

(74) Agents: COCKINGS, Orville et al.; International Coordinator, Rm. 1G112R, Telcordia Technologies, Inc., 445 South Street, Morristown, NJ 07960–6438 (US).

(81) Designated States: CA, JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND SYSTEM FOR SECURING WAVELENGTH DIVISION MULTIPLEX SYSTEMS



(57) Abstract

A system and method for securing DWDM networks (810) which includes adding background noise to a level up to the larger crosstalk signal or the background channel noise (e.g., amplified spontaneous emission level). The system comprises a white noise generator (821) appropriately placed so that any leaked signals are masked by the white noise generated. Accordingly, only the signals intended to be dropped are recoverable because all other signals would not be recoverable from the background white noise.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Method and System for Securing Wavelength Division Multiplex Systems

RELATED APPLICATIONS

The priority date for this Utility Patent Application is established by Provisional Patent Application Number 60/108,127, for which the filing date was November 12, 1998 and the application was entitled "Method and System for Securing Wavelength Division Multiplex Systems".

FIELD OF THE INVENTION

This invention relates to Dense Wavelength Multiplex Systems (DWDMs) and specifically to securing information or channels in these systems.

BACKGROUND OF THE INVENTION

Dense Wavelength Division Multiplex (DWDM) technology has provided a cost-effective solution to fiber exhaust in communications networks by increasing the data throughput of the network without requiring the installation of new fiber and is the enabling technology for the emerging all optical networking. In a DWDM system each of several input signals enter a DWDM node or network element and is assigned or converted to a specific wavelength, typically, in the 1550 nanometer (nm) band. After wavelength conversion each individual signal wavelength or channel is then multiplexed by wavelength division multiplexing and transmitted onto the same fiber. Consequently, a single fiber carries more than one wavelength. In fact each wavelength carried by a DWDM system may be considered a virtual fiber.

In order for DWDM technology to be truly viable as a network solution, DWDM systems must be secure. As opposed to real fibers, the signal carried on the virtual fibers of DWDM systems may be susceptible to eavesdropping. In DWDM systems different channels travel through the same fiber and the same components. As a result of crosstalk, nonlinearity, etc., at the receiving end, there is a residual of signal(s) from other channels that can be isolated, amplified, and detected.

The potential for eavesdropping may be better appreciated by reference to FIG. 1 where there is depicted a receiving node 100 in a DWDM network. Receiving node 100 may be an optical demultiplexer or add drop multiplexer, a wavelength converter, or an optical cross–connect that serves as a drop off or interchange point for one or more channels. FIG. 2 shows, on a logarithmic scale, the optical spectrum of channel 10 in FIG. 1 as it dropped from node 100. As FIG. 2 shows, although the goal was to drop only channel 10 channel 11 is clearly visible. In FIG. 3 I used a notch filter to reduce the optical signal to noise ratio (OSNR) for channel 10. As FIG. 3 shows channel 11 is still present with enough power to be recoverable. In fact, in FIG. 4 I have turned off the channel 10 transmitter and as FIG. 4 shows there is a significant amount of residual power still present from channel 11. I have also achieved similar results shown in FIG. 4 by introducing a second filter to attenuate channel 10 in the received spectrum. In either case, in FIG. 4, channel 11 is leaked with large enough OSNR to be recoverable after optical amplification. I have achieved better than 20 dB OSNR for the leaked signal for this particular optically amplified DWDM system. I expect better eavesdropping performance (larger OSNR than 20 dB for the leaked signal)

for DWDM systems without the amplified stimulated emission (ASE) associated with the optical amplification process. Accordingly, the user of channel of 10 may be able to recover channel 11 without the network operator ever knowing of the breach in security. On another level, residual power from each channel may be available on all the channels thereby providing for security akin to having a party line.

Of utility then would be a method and system for securing DWDM networks against potential eavesdropping.

SUMMARY OF THE INVENTION

My invention is a method and system for securing DWDM networks by introducing noise into the fiber channel or cable up to the level of cross-talk (leakage) or ASE noise, which ever is larger, so that unauthorized recovery of channels is prevented or not permitted.

In accordance with my invention a white noise source inputs white noise into the fiber channel up to amplified spontaneous emission level so that only the signal intended to be dropped or terminated can be recovered. In accordance with my invention the added noise masks the leaked signal without affecting the performance of the channel intended to be dropped or terminated.

By using only a noise source the network is secured against eavesdropping without the need of any sophisticated monitoring or processing software. Accordingly, a DWDM system designed in accordance with my invention will not incur a substantial increase in cost.

In one aspect of my invention the noise source is included as part of the DWDM node at the point multiwavelength signal is being received, i.e., at the point within the equipment before the multiwavelength signal is optically demultiplexed. Although the noise can be injected anywhere along the path of the mutiwavelength signals, it is most effective if injected at the receiving end.

In another aspect of my invention the noise source is coupled onto the fiber after the optical demultiplexer and just before the single channel optical signal is being handed over. In this case only the channels that have to be secure get the noise injection. In accordance with this aspect of invention DWDM systems that have been already deployed may be protected by my invention.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustratively depicts a receiving node in a DWDM network;

FIG. 2 is a spectral plot of a received channel that is dropped from the DWDM node of FIG. 1, channel 11 appears as cross-talk in the spectral plot of Figure 2;

FIG. 3 is a spectral plot of the spectrum in FIG. 2 after filtering;

FIG. 4 depicts the leaked channel after channel 10 in FIG. 3 is turned off or after a second filter is applied to FIG. 3;

FIG. 5 depicts the optical spectrum of the dropped channel with white noise added in accordance with my invention;

FIG. 6 illustratively depicts a node in a secure DWDM network designed in accordance with an aspect of my invention;

FIG. 7 illustratively depicts a secure DWDM network in accordance with another aspect of my invention; and

FIG. 8 illustratively depicts an optical cross–connect node in a multiwavelength network implemented in accordance with my invention.

DETAILED DESCRIPTION OF THE INVENTION

Turning now to FIG. 6, there is illustratively depicted a receiving node in a DWDM network that is dropping signals. In accordance with my invention a white noise source 610 may be placed at some point before a DWDM receiving node 620 as depicted in FIG. 6. The white noise source 610 includes a white noise generator 612 and coupler 613. In accordance with this aspect of my invention white noise is added to all the channels on fiber 615 at approximately detail A by the same source 610 or, specifically, by white noise generator 612.

The spectrum that results on channel 10 is illustratively shown in FIG. 5. As FIG. 5 shows, white noise is added only up to the amplified spontaneous emission level of the amplifiers deployed in the system. As FIG. 5 also shows, the added noise masks channel 11 while allowing recovery of channel 10. Note also that although FIG. 5 clearly shows channel 11, on an actual oscilloscope trace channel 11 would not at all be identifiable, i.e., it's presence is not detectable at channel 10. Accordingly the intended recipient or carrier of channel 10 is not able to recover channel 11. Therefore, a DWDM system employing my invention in this manner allows the network operator to provide security. As such, by my invention DWDM systems already deployed can be secured by the network provider without any redesign or reengineering of these systems. This is the case because the

noise or security code is added to fiber 615 at detail A either before or after the signal or information is internal to DWDM node or supplier equipment 620 and not in the node or any supplier equipment.

In accordance with another aspect of my invention white noise may be coupled only onto the channels being dropped before those signals are handed off to another carrier or a customer. Turning now to FIG. 7, there is depicted a secure WDM node 710 of a DWDM system designed in accordance with this aspect of my invention. In FIG. 7, incoming signals on fiber span 705 are demultiplexed at WDM node 710 by optical demultiplexer 711. One of the signals that is demultiplexed is dropped at node 710 and is illustratively depicted as signal or channel 10. Typically, optical signal or channel 10 is handed over to another carrier. As can be seen by reference to FIG. 2 when channel 10 is dropped, other channels, such as channel 11, are leaked, thereby allowing for eavesdropping. However, in accordance with this aspect of my invention noise generator 712 residing in node 710 injects white noise onto the dropped signal of channel 10 after the signal is demultiplexed by demultiplexer 711 but before channel 10 exits node 710. Accordingly, the spectrum shown in FIG. 5 results. In the absence of my invention the intended recipient or carrier of channel 10 has access to the signal leaked from channel 11. That leaked signal can be filtered, optically amplified, and recovered using conventional techniques. The particular application of my invention depicted in FIG. 7 may be particularly advantageous in scenarios where the owner of node 710 is precluded from adding noise generator 712 to fiber 705 owing to regulatory considerations.

At node 710 the inverse operation to demultiplexing may also take place. That is, signal 110 enters node 710 so as to be multiplexed and transmitted to node 790 . At node 710 the multiplexing operation is carried out by wavelength division multiplexer 720. The multiplexed signal from multiplexer 720 is then coupled on fiber span 780 for transmission to node 790. At node 790 an operation similar to that which took place at node 710 also occurs, i.e., signals are added and dropped as required by customers. As such, by addition of a noise source in accordance with my invention only the channels intended to be dropped are decipherable by their respective recipient. Accordingly, by my invention a low cost solution is provided which prevents eavesdropping in DWDM networks.

My security method is also particularly advantageous in optical-cross connect nodes of a multiwavelength optical network because security can be done where it is most convenient. For example, and with reference to FIG. 8, an optical cross–connect 810 that is being used to groom traffic from several DWDM nodes 820 may also be used to secure traffic to and from the nodes 820. Specifically, after the signals are de–multiplexed in cross–connect 810 a white noise generator 821 injects noise onto the signal up to the ASE level. Although FIG. 8 illustratively depicts the placement of noise generator 821 after the incoming signals to cross–connect 810 are de–multiplexed, the addition of noise may also be done right at the input of the cross–connect multiplexers. This implementation is depicted by the placement of noise generator 822 in FIG. 8. As discussed above the signal or information would be secure against eavesdropping.

Although the above description is directed to DWDM systems, i.e., systems have optical amplifiers, my invention is also applicable to systems not having optical amplifiers. In those systems noise would be added only up to the level necessary to mask leaked channels.

The above description is exemplary of my invention. Numerous modifications and variations may be made by those skilled in the art without departing from the scope and spirit of my invention.

CLAIMS

1. An optical communications system in which first and second virtual fibers are associated with first and second carrier wavelengths in a single optical fiber as a multiplexed signal, said system including:

a demultiplexing node for accepting as input said multiplexed signal, and for separating from same the signal associated with said first carrier wavelength as an output to be dropped or further transmitted; and

a noise generator for adding a predetermined noise level signal so as to mask the signals associated with said second carrier wavelength.

2. An optical communications system as defined in claim 1 in which said noise generator generates white noise.

3. An optical communications system as defined in claim 1 in which the predetermined noise level is approximately equal to the signal coupled from said second carrier wavelength signal.

4. An optical communications system as defined in claim 1 in which said noise generator adds noise to the multiplexed input signal.

5. An optical communications system as defined in claim 1 in which said noise generator adds noise to the demultiplexed output signal associated with said first carrier wavelength.

6. An optical communications system as defined in claim 1 in which the signals associated with said second carrier wavelength are also separated from the multiplexed signal by the demultiplexing node as an output to be further transmitted, and the signals associated with said first carrier wavelength are also masked by said noise level signal.

7. An optical communication system having a plurality of wavelengths, each wavelength within the plurality of wavelengths representing a channel in said system, said system comprising:

a first node having a wavelength division multiplexer and a wavelength division demultiplexer;

a second node coupled said first node by a fiber; and

a noise source coupled to said first node such that a noise signal is added to the channels prior said first node wavelength division demultiplexer such that only the channels meant to be demultiplexed at said second node are decipherable.

8. The system in accordance with claim 7 wherein said noise source is externally coupled to said first node.

9. The system in accordance with claim 7 wherein said noise source is internally coupled to said first node.

10. The system in accordance with claim 9 wherein said first node is an optical cross connect.

11. A method for securing an optical communication system having a plurality of wavelengths, each wavelength within the plurality of wavelengths representing a channel in the system, the system including a plurality of WDM nodes interconnected by fiber cable, said method comprising the step of introducing noise into the fiber cable so that only the channel intended to be dropped at each node of the plurality of nodes can be recovered.

12. The method in accordance with claim 11 wherein said step of introducing noise comprises the substep of coupling white noise onto the fiber cable up to the amplified spontaneous emission level on the fiber cable.

13. A method for preventing a signal on a first wavelength optical channel on a multichannel fiber optical cable from being detected on a second wavelength optical channel on the fiber optical cable, said method comprising the step of coupling white noise to all the channels on the fiber optical cable ip to the amplified spontaneous emission level on the fiber optical cable.

FIG. 1

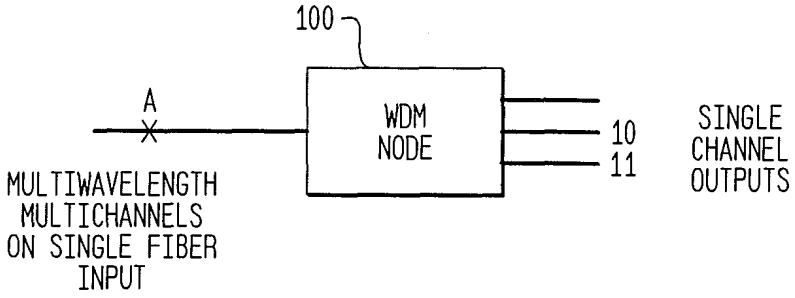

100
A
WDM
NODE
10
11
SINGLE
CHANNEL
OUTPUTS
MULTIWAVELENGTH
MULTICHANNELS
ON SINGLE FIBER
INPUT

FIG. 2

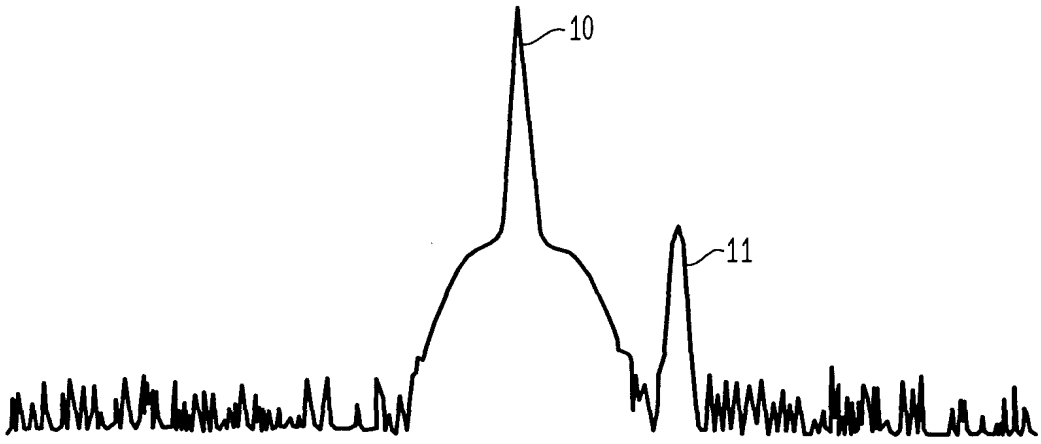

10
11

FIG. 3

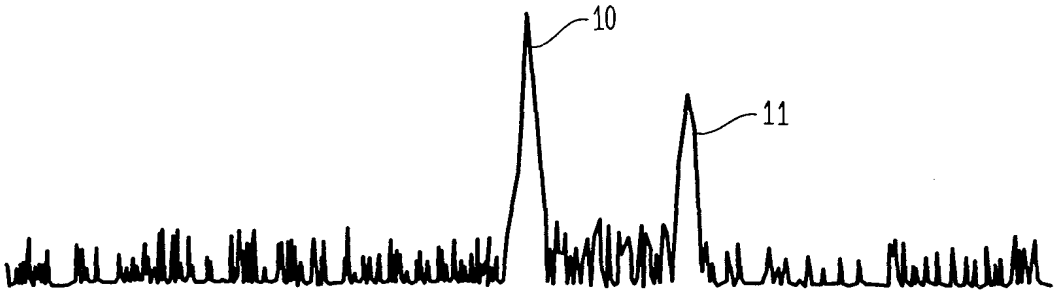


FIG. 4

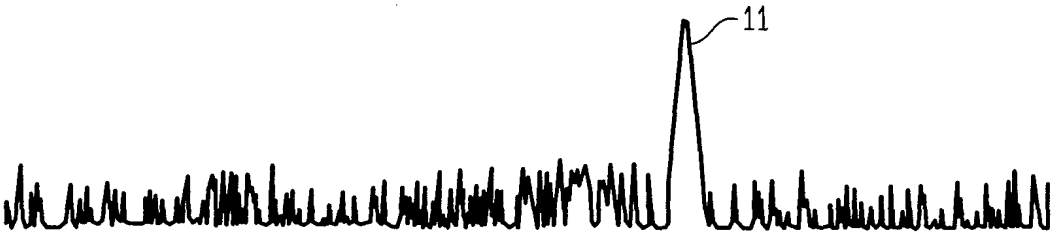


FIG. 5

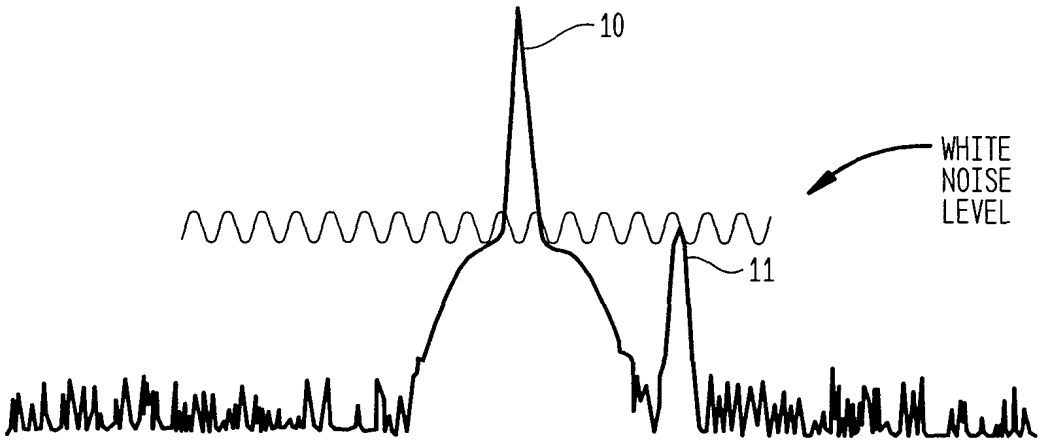


FIG. 6

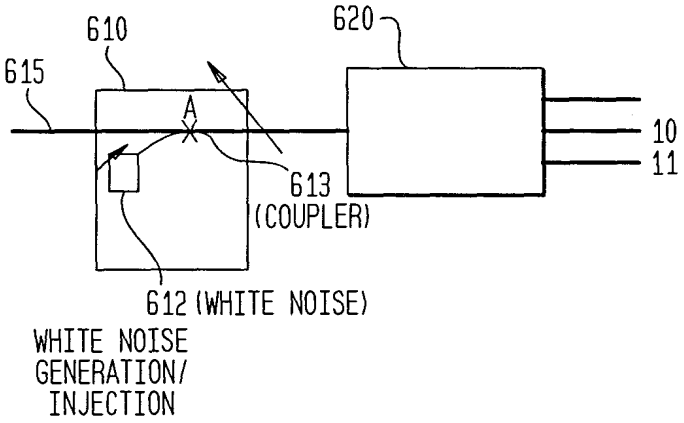

610
620
615
A
10
11
613
(COUPLER)
612 (WHITE NOISE)
WHITE NOISE
GENERATION/
INJECTION

FIG. 7

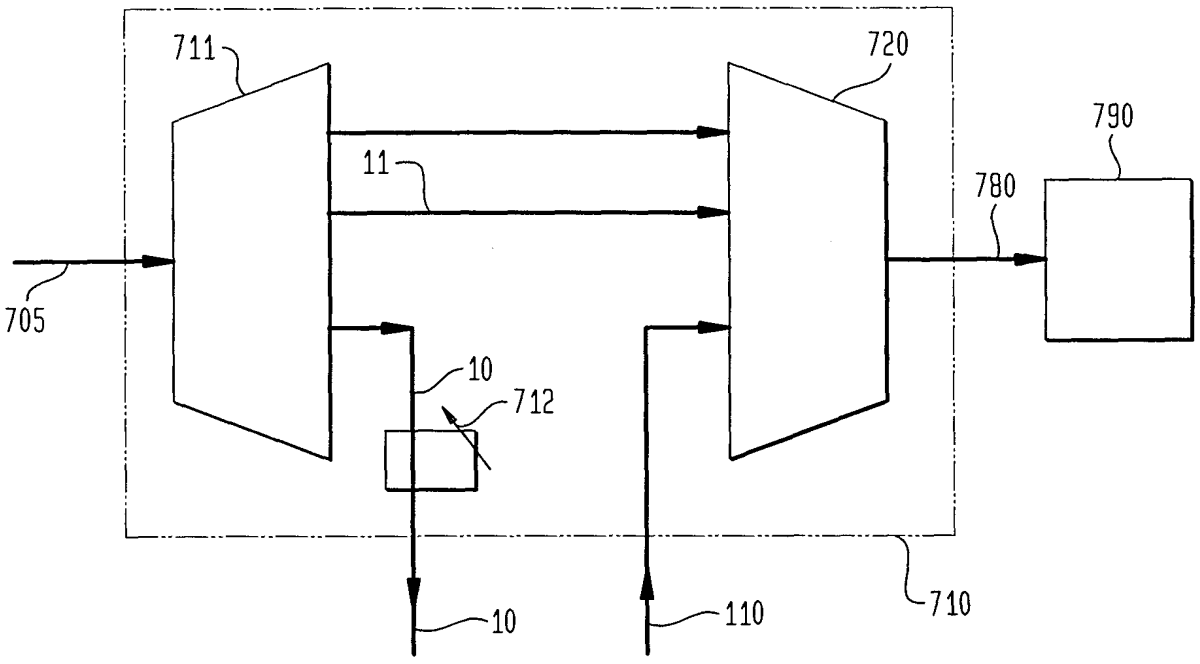
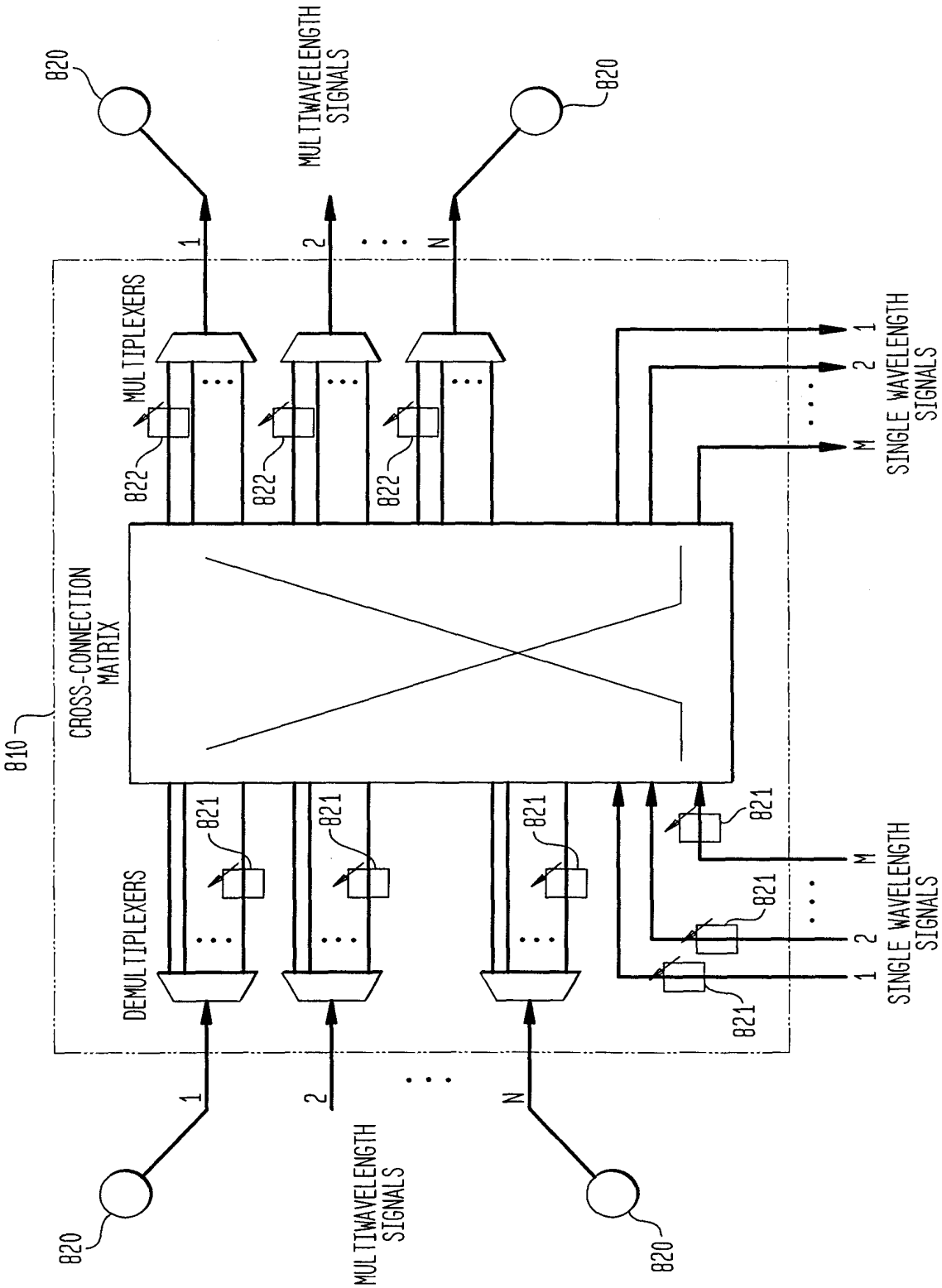

711
720
790
11
780
705
10
712
10
110
710

FIG. 8


820
MULTIWAVELENGTH SIGNALS
820
1
2
N
MULTIPLEXERS
822
822
822
SINGLE WAVELENGTH SIGNALS
1
2
M
810
CROSS-CONNECTION MATRIX
821
821
821
821
821
DEMULTIPLEXERS
1
2
N
820
MULTIWAVELENGTH SIGNALS
820
SINGLE WAVELENGTH SIGNALS
1
2
M

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/26529

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04J 14/00, 14/02; H04K 1/02, 1/10
US CL :359/127, 112, 161, 124
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 359/127, 112, 161, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

IEEE DATABASE
search terms: secure communication, jaming, masking

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	ELMIRGHANI, J.M.H. Communication Using Chaotic Masking IEE Colloquium on Exploiting Chaos in Signal Processing. 1994. pages 12/1-12/6	1-13
Y	ELMIRGHANI, J.M.H. Point-to-point and Multi-user Communication Based on Chaotic Sequences. IEEE International Conference on Communications. June 1995. Vol. 1. pages 582 - 584	1-13
Y	ELMIRGHANI, J.M.H. Data Communication via Chaotic Encoding and Associated Security Issues. IEEE Global Telecommunications Conference. November 1995. Vol. 2. page 1188-1192	1-13

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 27 FEBRUARY 2000	Date of mailing of the international search report 04 APR 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Jason Chan Telephone No. (703) 305-4729

Form PCT/ISA/210 (second sheet) (July 1998)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/26529

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	LEE, J. Secure Communication Using Chaos. IEEE Global Telecommunications Conference. November 1995. Vol. 2. pages 1183-1187	1-13
Y	AL-BAYATI, A.K.S. A Novel Design of a Speech Security System for Telephone Channels. 6th Mediterranean Electrotechnical Conference. May 1991. Vol.1. pages 456 - 459	1-13
Y,P	US 5,923,667 A (POIRAUD et. al.) 13 July 1999, figures 1, 2, 5	1, 4, 6, 9
Y	US 3,737,584 A (KANEKO et al) 05 June 1973, col. 2, lines 54-67, figure 1	1, 2, 6, 7, 8, 11-13